

WHAT IS CLAIMED IS:

1 1. A storage system comprising:
2 an interface to a host computer;
3 a storage controller including a central processing unit that conducts an I/O
4 operation and management operation;
5 a memory to store an operation log, the operation log being used to record a
6 description of a management operation and a corresponding timestamp;
7 storage volumes defined by at least one storage device; and
8 an attribute for each of the storage volumes stored in the memory,
9 wherein write access to each of the storage volumes is dependent on the
10 attribute.

1 2. The storage system of claim 1 wherein the attribute identifies a storage
2 volume as at least one of write protected, offline, and normal.

1 3. The storage system of claim 1 wherein the memory is a non-volatile
2 random access memory.

1 4. The storage system of claim 1 wherein the storage device is a hard disk
2 drive, the storage system having at least 10 hard disk drives, the storage system being a disk
3 array unit.

1 5. The storage system of claim 1 further comprising a management
2 interface connected to a console, the console receiving the operation log from the storage
3 system.

1 6. The storage system of claim 5 wherein the management interface is
2 further connected to the console via a communication network, wherein the console receives
3 the operation log over the communication network.

1 7. The storage system of claim 1, wherein a write protect period is
2 associated with each of the storage volumes identified by the attribute as write protected.

1 8. The storage system of claim 1 wherein the operation log comprises:
2 a first log for system management operations; and
3 a second log for logical volume operations.

1 9. The storage system of claim 8 wherein the second log comprises
2 volume operations for each of the storage volumes depending on the attribute.

1 10. The storage system of claim 8 wherein the operation log further
2 comprises an I/O operation log for recording read access information for each of the storage
3 volumes.

4 11. A method of assuring genuineness of data maintained on a storage
5 subsystem having a storage controller and a plurality of storage disks, the method
6 comprising:

7 maintaining a first log and second log;

8 recording management operations of the storage subsystem and corresponding
9 timestamps to the first log;

10 identifying a write protect attribute and write protect period for a logical
11 volume;

12 recording management operations of the logical volume and corresponding
13 timestamps to the second log depending on the write protect attribute and write protect
14 period;

15 denying write access to the logical volume to a host based on the write protect
16 attribute and write protect period of the logical volume; and

17 providing information from the first log, second log, or a combination of the
18 first and second log to a console.

1 12. The method of claim 11 wherein the first log and second log are stored
2 in non-volatile random access memory.

1 13. The method of claim 11 wherein the write protect attribute and write
2 protect period are stored in the non-volatile random access memory.

1 14. The method of claim 11 wherein the information is provided over a
2 communication network to a user on the console.

1 15. The method of claim 11 further comprising:
2 specifying a threshold for sequential read access to the logical volume;
3 monitoring read access to the logical volume; and

4 recording information and corresponding timestamp to the second log if the
5 threshold is exceeded.

1 16. The method of claim 15 wherein the threshold applies to all logical
2 volumes of the storage subsystem.

1 17. A computer program product stored on a computer-readable storage
2 medium for assuring genuineness of data maintained on a storage subsystem having a storage
3 controller and a plurality of storage disks, the computer program product comprising:

4 code for maintaining a first log and second log;

5 code for recording management operations of the storage subsystem and
6 corresponding timestamps to the first log;

7 code for identifying a write protect attribute and write protect period for a
8 logical volume;

9 code for recording management operations of the logical volume and
10 corresponding timestamps to the second log depending on the write protect attribute and
11 write protect period;

12 code for denying write access to the logical volume to a host based on the
13 write protect attribute and write protect period of the logical volume; and

14 code for providing information from the first log, second log, or a combination
15 of the first and second log to a console.

1 18. The computer program product of claim 17 further comprising:

2 code for specifying a threshold for sequential read access to the logical
3 volume;

4 code for monitoring read access to the logical volume; and

5 code for recording information and corresponding timestamp to the second log
6 if the threshold is exceeded.